IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

JULIE TAPIA, on behalf of herself and all others similarly situated,	)	
Plaintiff,	)	**CIVIL ACTION NO.: _____**
v.	)	**CLASS ACTION COMPLAINT**
HOSPITALITY STAFFING SOLUTIONS, LLC, a Georgia limited liability company,	)	**JURY TRIAL DEMANDED**
Defendant.	)	

CLASS ACTION COMPLAINT

Julie Tapia ("Ms. Tapia" or "Plaintiff"), individually and on behalf of all others similarly situated, alleges the following against Hospitality Staffing Solutions, LLC ("HSS" or "Defendant"), based upon personal knowledge, where applicable, information and belief, and the investigation of counsel:

SUMMARY OF ACTION

1. Plaintiff brings this class action on her own behalf and on behalf of all past and current employees (collectively, "employees") of HSS whose private, sensitive Personal Identifying Information ("PII") and Financial Account

Information ("FAI"), was compromised as a direct result of HSS's failure to take adequate and reasonable measures to protect its network and computer systems.

2. Despite repeated warnings from security experts as well as the federal government about the risk of data breaches and ransomware attacks, HSS failed to comply with industry standards and its statutory and common law duties to protect the PII and FAI of its employees.

3. Between approximately March 2, 2023, and June 2, 2023, the PII and FAI of at least 104,660 HSS employees was accessed by an unauthorized third party due to HSS's severely inadequate security practices (the "Data Breach"). HSS's actions and omissions left its employees' highly sensitive PII and FAI, including, but not limited to, names, social security numbers, and driver's license numbers ("Personal Identifying Information"), as well as accountholder or cardholder names, financial account numbers, credit or debit card numbers, expiration dates, security codes, access codes, passwords and/or PIN numbers for the accounts ("Financial Account Information"), exposed and accessible for hackers to steal for three months. As a result, Plaintiff and Class Members have suffered injuries, including financial fraud, lost or diminished value of their PII and FAI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from financial fraud, identity theft, tax fraud, and/or other unauthorized use of their PII and FAI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of

the Data Breach, including but not limited to lost time, and (iv) the continued and certainly increased risk to their PII and FAI.

4. As far as Plaintiff knows, her PII and FAI and other sensitive information in HSS's possession remains unencrypted and available for more unauthorized third parties to access and abuse and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect it.

5. Plaintiff seeks to recover damages and equitable relief on behalf of herself and all other similarly situated persons in the United States as a result of the HSS Data Breach.

JURISDICTION AND VENUE

6. This Court has original jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C §1332 (d). The matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, at least one member of the proposed class (Ms. Tapia) is of diverse citizenship from the Defendant, and there are more than 100 putative class members.

7. This Court has personal jurisdiction over Defendant because it maintains its principal place of business within this District, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia.

8. Venue is proper under 18 U.S.C. § 1391(b) because Defendant's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

PARTIES

9. Plaintiff Julie Tapia is an adult citizen of Alabama who resides in Jefferson County, Alabama.

10. Defendant Hospitality Staffing Solutions, LLC is a limited liability company organized under the laws of Delaware, with its principal place of business located at 1117 Perimeter Center West, Suite E401, Atlanta, Georgia. HSS is a corporate citizen of both Delaware and Georgia. HSS is wholly owned by HS Solutions Corporation, which is a Delaware corporation.

11. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known, including the members of the LLC.

12. HSS is a staffing and employment company that serves the hospitality and hotel industry throughout the United States. Upon information and belief, HSS is the largest staffing company in the United States focused on hospitality,

generating hundreds of millions of dollars in revenue and employing thousands of people. HSS has 97 offices across 37 states and provides contract or temporary workers to perform housekeeping or janitorial services on behalf of the HSS customer at the customer's location. HSS's outsourcing service entails HSS assuming the responsibility for the management, recruitment, staffing, and supervision of workers at a customer's facility. In exchange for such services, HSS is paid a fixed rate for work performed and/or a billing rate of its assigned employees. As such, HSS gathers and stores vast amounts of its employees' private, sensitive information.

STATEMENT OF FACTS

HSS Acquires and Stores the PII and FAI of Plaintiff and Class Members

13. Plaintiff and Class Members employed by HSS were required to provide sensitive and confidential information, including (but not limited to) their names, addresses, phone numbers, email addresses, Social Security numbers, driver's license numbers, and full payment account information to be used in the payroll process.

14. This vast trove of sensitive information can be used to commit a myriad of financial crimes against a person.

15. By obtaining, collecting, and storing the PII and FAI of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known

that it was responsible for protecting the PII and FAI from unauthorized disclosure.

16. Plaintiff and Class Members relied on—and expected—this sophisticated Defendant to keep their PII and FAI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand HSS implement security to safeguard their PII and FAI from further unauthorized access.

The Data Breach

17. On or about August 1, 2023, Defendant sent Plaintiff and Class Members a Notice of Data Incident. A copy of the template notice letter HSS provided to the Maine Attorney General is attached as Exhibit A.

18. The letter explained:

> ***What Happened?*** *On June 2, 2023, we discovered that an unauthorized third party accessed our network environment. We immediately took steps to secure our systems and initiated an investigation to determine the nature and scope of the incident. Our investigation determined that files containing personal information were accessed by the unauthorized third party.*
>
> ***What Information Was Involved?*** *We reviewed the contents of the files involved to determine what information may have been accessible to the unauthorized individual(s). Our review identified files that included your name and one or more of the following: Social Security number, driver's license number, and/or financial account number.*

19. HSS has also notified various regulatory agencies and state Attorneys general of the Data Breach.

20. HSS has admitted in its notice letter that the PII and FAI of the Plaintiff and Class Members was accessed by an "unauthorized third party." However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

21. The unencrypted PII and FAI of Plaintiff and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members.

22. Upon information and belief, a ransomware group that calls themselves "Akira" claims to have stolen and made over 1.3 terabytes of HSS's company data available on the dark web.

23. "Unauthorized third parties" do not illegally access the valuable PII and FAI other 104,000 people without a nefarious—likely criminal—purpose.

24. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was

maintaining for Plaintiff and Class Members, causing the exposure of PII and FAI for more than 104,000 individuals.

25. There are numerous data and network security measures that HSS should have implemented to prevent and detect hacking attacks, including the attack that resulted in the Data Breach.

26. Given that Defendant was storing the PII and FAI of more than 104,000 individuals, Defendant could and should have implemented additional security measures to prevent and detect hacking or other cybersecurity attacks.

Securing PII and FAI and Preventing Breaches

27. Defendant could have prevented this Data Breach by properly securing and encrypting the files, networks and servers containing the PII and FAI of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially old data from former employees.

28. Defendant's negligence in failing to safeguard the PII and FAI of Plaintiff and Class Members is exacerbated by Defendant's disregard of the repeated warnings and alerts regarding protecting and securing sensitive data that have been publicized by both governmental agencies and the cybersecurity industry.

29. Defendant had actual knowledge of these public warnings and of the threat of cyberattacks against it, but still failed to take the appropriate actions to protect the valuable PII and FAI of its employees.

30. Defendant had actual knowledge of other large employers who experienced similar cyberattacks prior to allowing this Data Breach to occur.

31. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII and FAI of Plaintiff and Class Members from being compromised.

32. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[1] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[2]

33. The ramifications of Defendant's failure to keep secure the PII and FAI of Plaintiff and Class Members are long lasting and severe. Once PII and FAI are stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

---

[1] 17 C.F.R. § 248.201 (2013).
[2] *Id.*

34. The PII and FAI compromised in the Data Breach is highly valuable to criminals and is now being used to commit identity theft and/or financial fraud against Plaintiff and Class Members.

35. However, the full extent of the fraudulent activity resulting from the Data Breach may not come to light for years.

36. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII and FAI.

37. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's file servers, amounting to potentially tens or hundreds of thousands of individuals detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

38. To date, Defendant has offered Plaintiff and Class Members only one year of credit monitoring and identity theft detection through a single credit bureau, Equifax. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII and FAI at issue here.

39. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII and FAI of Plaintiff and Class Members.

Plaintiff Julie Tapia's Experience

40. Ms. Tapia applied for employment with HSS in 2019 and despite only briefly working for HSS in 2019, she was required to provide HSS with all the aforementioned PII and FAI as a prerequisite to her potential employment.

41. Despite Ms. Tapia not working for HSS for the past three (3) years, HSS is still storing the sensitive PII and FAI she provided to it in its internal computer systems and networks.

42. Ms. Tapia has always been careful to keep her PII private and secure.

43. As a result of her PII and FAI being compromised in the Data Breach, Ms. Tapia is now a victim of identity theft and financial fraud.

44. Specifically, Ms. Tapia has received alerts that an identity thief has attempted to open multiple financial accounts in her name without her authorization.

45. As a result of this fraudulent activity, Ms. Tapia also received multiple "hard" credit inquiries on her credit report, which negatively affected her credit score.

46. Ms. Tapia received Defendant's Notice of Data Incident, dated August 1, 2023, on or about that date. The notice stated that Plaintiff's PII and FAI were contained in files accessed during the Data Breach.

CLASS ALLEGATIONS

47. Plaintiff brings this nationwide class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

48. The Nationwide Class that Plaintiff seek to represent is defined as follows:

> All individuals residing in the United States who were notified by HSS that their personal information was or may have been compromised in the Data Breach experienced by HSS on or around August 1, 2023 (the "Nationwide Class").

49. Alternatively, or in addition to the Nationwide Class claims, Plaintiff brings these claims on behalf of herself and on behalf of Subclasses of individuals and entities residing in the State of Alabama. The Alabama Subclass is defined as follows:

> All individuals residing in the State of Alabama who were notified by HSS that their personal information was or may have been compromised in the Data Breach experienced by HSS on or around August 1, 2023 (the "Alabama Subclass").

50. Collectively, the Nationwide Class and Alabama Subclass are referred to herein as the "Class or "Classes."

51. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

52. Plaintiff reserves the right to modify or amend the definition of the proposed Classes before the Court determines whether certification is appropriate.

53. Numerosity, Fed R. Civ. P. 23(a)(1): The Classes are so numerous that joinder of all members is impracticable. Defendant has identified over one hundred thousand current and former applicants or employees whose PII and FAI may have been improperly accessed in the Data Breach, and the Classes are apparently identifiable within Defendant's records. Defendant advised the Maine Attorney General that the Data Breach affected 104,660 individuals.

54. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII and FAI of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the PII and FAI of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the PII and FAI of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII and FAI of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and FAI had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII and FAI had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and FAI of Plaintiff and Class Members;

k. Whether Defendant breached its implied contracts with Plaintiff and the Class Members by failing to safeguard the PII and FAI of Plaintiff and Class Members;

l. Whether Defendant invaded the privacy of Plaintiff and Class Members by failing to safeguard the PII and FAI of Plaintiff and Class Members;

m. Whether Defendant breached the confidence of Plaintiff and Class Members by failing to safeguard the PII and FAI of Plaintiff and Class Members

n. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

o. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

p. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

55. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII and FAI compromised as a result of the Data Breach, due to Defendant's misfeasance.

56. Policies Generally Applicable to the Classes: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiff.

57. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Classes and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

58. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds or thousands of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

59. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed

is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

60. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

61. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

62. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure and safeguard the PII and FAI of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

63. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

64. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and FAI;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and FAI;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII and FAI had been compromised;

g. Whether Defendant failed to implement and maintain reasonable

security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and FAI of Plaintiff and Class Members; and,

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE/WANTONESS
(On Behalf of Plaintiff and the Classes)

65. Plaintiff realleges the factual allegations contained in paragraphs 1 through 64 as if fully set forth herein, and further alleges as follows:

66. As a condition of their employment with Defendant or a company it acquired, Plaintiff and the Class were obligated to provide Defendant or a company it acquired with certain PII and FAI, including their names, Social Security numbers, driver's license information, and payment account information.

67. Plaintiff and the Class entrusted their PII and FAI to Defendant or a company it acquired on the premise and with the understanding that Defendant or a company it acquired would safeguard their information, use their PII and FAI

for business purposes only, and/or not disclose their PII and FAI to unauthorized third parties.

68. Defendant has full knowledge of the sensitivity of the PII and FAI and the types of harm that Plaintiff and the Class could and would suffer if the PII or FAI were wrongfully disclosed.

69. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII or FAI of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

70. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII and FAI of Plaintiff and the Class in Defendant's possession was adequately secured and protected.

71. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former employees' PII and FAI it was no longer required to retain pursuant to regulations.

72. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII and FAI of Plaintiff and the Class.

73. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant or a company it acquired with their confidential PII and FAI, a necessary part of potential employment with Defendant or a company it acquired.

74. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

75. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices, procedures, and protocols.

76. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices, procedures, and protocols. Defendant knew or should have known of the inherent risks in collecting and storing the PII and FAI of Plaintiff and the Class, the critical importance of providing adequate security of that PII and FAI, and the necessity for encrypting PII and FAI stored on Defendant's systems and networks.

77. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII and FAI of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

78. Plaintiff and the Class had no ability to protect their PII and FAI that was in, and possibly remains in, Defendant's possession.

79. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

80. Defendant had and continues to have a duty to adequately disclose that the PII and FAI of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and FAI by third parties.

81. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and FAI of Plaintiff and the Class.

82. Defendant has admitted that the PII and FAI of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

83. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII and FAI of Plaintiff and the Class during the time the PII and FAI was within Defendant's possession, care, custody, or control.

84. Defendant improperly and inadequately safeguarded the PII and FAI of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

85. Defendant failed to heed industry and government warnings and alerts to provide adequate safeguards to protect the PII and FAI of Plaintiff and the Class in the face of increased risk of theft.

86. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to have appropriate security protocols and procedures in place to detect and prevent dissemination of applicants' and employees' PII and FAI.

87. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove former employees' PII and FAI it was no longer required to retain pursuant to regulations.

88. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

89. But for Defendant's wrongful, negligent, and wanton breach of duties owed to Plaintiff and the Class, the PII and FAI of Plaintiff and the Class would not have been compromised.

90. There is a close causal connection between Defendant's failure to implement security measures to protect the PII and FAI of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII and FAI of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII and FAI by adopting, implementing, and maintaining appropriate security measures.

91. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

92. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and FAI and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII and FAI it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

93. Defendant's violation of Section 5 of the FTC Act constitutes negligence per se.

94. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

95. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

96. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII and FAI; (iv) out-of-pocket expenses associated with the prevention, detection,

and recovery from identity theft, financial or tax fraud, and/or unauthorized use of their PII and FAI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from financial or tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and FAI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and FAI of Plaintiff and the Class; and (viii) present and future costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII and FAI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

97. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

98. Additionally, as a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII and FAI, which remain in

Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and FAI in its continued possession.

99. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Classes)

100. Plaintiff re-alleges the factual allegations contained in paragraphs 1 through 64 as if fully set forth herein, and further alleges as follows:

101. Federal and state statutory law and applicable regulations set forth and otherwise establish duties in the industry that were applicable to HSS and with which HSS was obligated to comply at all relevant times hereto.

102. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair ... practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by businesses such as Defendant of failing to use reasonable measures to protect PII and FAI.

103. Subsection 8-38-3(a) of the Alabama Data Breach Notification Act of 2018 imposes a clear duty on entities like HSS to protect PII and FAI: "Each covered entity and third-party agent shall implement and maintain reasonable

security measures to protect sensitive personally identifying information against a breach of security."

104. HSS violated these duties and others by failing to secure, safeguard and protect the Plaintiff's and Class Members' PII and FAI, which resulted in an unauthorized disclosure of the Plaintiff's and the Class Members' PII and FAI.

105. HSS was also prohibited by the FTC Act from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for sensitive personal information is an "unfair practice" in violation of the FTC Act. Various FTC publications and orders also form the basis of HSS's duty.

106. HSS violated Section 5 of the FTC Act by failing to maintain reasonable and appropriate data security for the PII and FAI it stores.

107. The unauthorized disclosure of the Plaintiff's and Class Members' PII and FAI at issue in this action was exactly the type of conduct that the legislation referenced above was intended to prohibit, and the harm at issue in this case that has been suffered by the Plaintiff and Class Members is the type of harm the legislation referenced above was intended to prevent.

108. Plaintiff and Class Members, as owners of the sensitive personally identifying information that HSS failed to protect, fall within the class of persons

the FTC Act, the Alabama Data Breach Notification Act, and similar statutes were intended to protect.

109. The harm suffered and that may be suffered in the future by the Plaintiff and Class Members is the same type of harm the FTC Act, the Alabama Data Breach Notification Act of 2018, and similar statutes were intended to guard against.

110. As a direct and proximate result of HSS' violation of the FTC Act, the Alabama Data Breach Notification Act of 2018, and similar statutes, the Plaintiff and Class Members were damaged in the form of, without limitation, financial fraud, identity theft, loss of time monitoring credit reports and financial accounts and placing credit freezes, expenses for credit monitoring and insurance, expenses for periodic credit reports, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and noneconomic harm.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Classes)

111. Plaintiff re-alleges the factual allegations contained in paragraphs 1 through 64 as if fully set forth herein, and further alleges as follows:

112. Defendant required Plaintiff and the Class to provide their personal information, including names and Social Security numbers, driver's license information, and FAI, as a condition of their potential employment.

113. As a condition of their potential employment with Defendant, Plaintiff and the Class provided their personal and financial information. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

114. Defendant manifested its intent to provide data security to Plaintiff and the Class as part of its employment agreements.

115. Plaintiff and the Class relied on Defendant's data security policies and procedures when they agreed to provide their PII and FAI to Defendant, and Plaintiff and the Class would not have provided such sensitive information to Defendant had Defendant not agreed to keep it secure and protected from cyberattacks.

116. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

117. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal and financial information and by failing to provide timely and accurate notice to them that personal and financial information was compromised as a result of the Data Breach.

118. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

119. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT IV
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Classes)

120. Plaintiff re-alleges the factual allegations contained in paragraphs 1 through 64 as if fully set forth herein, and further alleges as follows:

121. Plaintiff and the Class had a legitimate expectation of privacy to their PII and FAI and were entitled to the protection of this information against disclosure to unauthorized third parties.

122. Defendant owed a duty to its prospective, current, and former employees, including Plaintiff and the Class, to keep their PII and FAI contained as a part thereof, confidential.

123. Defendant failed to protect and released to unknown and unauthorized third parties the PII and FAI of Plaintiff and the Class.

124. Defendant allowed unauthorized and unknown third parties access to and examination of the PII and FAI of Plaintiff and the Class, by way of Defendant's failure to protect the PII and FAI.

125. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII and FAI of Plaintiff and the Class is highly offensive to a reasonable person.

126. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Class disclosed their PII and FAI to Defendant or a company it acquired as part of their employment or prospective employment with Defendant or a company it acquired, but privately with an intention that the PII and FAI would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their

belief that such information would be kept private and would not be disclosed without their authorization.

127. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

128. Defendant acted with a knowing state of mind when its permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

129. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class.

130. As a proximate result of the above acts and omissions of Defendant, the PII and FAI of Plaintiff and the Class was disclosed to third parties without authorization, causing Plaintiff and the Class to suffer damages.

131. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class in that the PII and FAI maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Class have no adequate remedy at law for the injuries in that a judgment

for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

132. As a direct and proximate result of Defendant's invasion of privacy, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT V
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Classes)

133. Plaintiff re-alleges the factual allegations contained in paragraphs 1 through 64 as if fully set forth herein, and further alleges as follows:

134. At all times during Plaintiff's and the Class's interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and the Class's PII and FAI that Plaintiff and the Class provided to Defendant or a company it acquired.

135. As alleged herein and above, Defendant's relationship with Plaintiff and the Class was governed by terms and expectations that Plaintiff's and the Class's PII and FAI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

136. Plaintiff and the Class employed by Defendant or a company it acquired provided Plaintiff's and the Class's PII and FAI to Defendant or a company it acquired with the explicit and implicit understandings that Defendant

or a company it acquired would protect and not permit the PII and FAI to be disseminated to any unauthorized third parties.

137. Plaintiff and the Class employed by Defendant or a company it acquired also provided Plaintiff's and the Class's PII and FAI to Defendant or a company it acquired with the explicit and implicit understandings that Defendant or a company it acquired would take precautions to protect that PII and FAI from unauthorized disclosure.

138. Defendant voluntarily received in confidence Plaintiff's and the Class's PII and FAI with the understanding that PII and FAI would not be disclosed or disseminated to the public or any unauthorized third parties.

139. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff's and the Class's PII and FAI was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and the Class's confidence, and without their express permission.

140. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and the Class have suffered damages.

141. But for Defendant's disclosure of Plaintiff's and the Class's PII and FAI in violation of the parties' understanding of confidence, their PII and FAI would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause

of the theft of Plaintiff's and the Class's PII and FAI as well as the resulting damages.

142. The injury and harm Plaintiff and the Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and the Class's PII and FAI. Defendant knew or should have known its methods of accepting and securing Plaintiff's and the Class's PII and FAI was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and the Class's PII and FAI.

143. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Class, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and FAI is used; (iii) the compromise, publication, and/or theft of their PII and FAI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, financial or tax fraud, and/or unauthorized use of their PII and FAI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from financial or tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and FAI, which remain

in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and FAI of current and former employees; and (viii) present and future costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII and FAI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

144. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

145. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

PRAYER FOR RELIEF

146. Wherefore, Plaintiff, on behalf of herself and on behalf of the proposed Class, requests that this Court award relief against Defendant as follows:

A. For an Order certifying the Class and appointing Plaintiff and her Counsel to represent such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse

and/or disclosure of the PII and FAI of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the PII and FAI of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the

confidentiality and integrity of the PII and FAI in Defendant's possession, care, custody, or control;

v. prohibiting Defendant from maintaining the PII and FAI of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and

securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII or FAI, as well as protecting the PII and FAI of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for

threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII or FAI to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses pursuant to O.C.G.A. Section 13-6-11, and as otherwise allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: August 17, 2023

Respectfully submitted,

/s/ MaryBeth V. Gibson
MaryBeth V. Gibson
Georgia Bar No. 725843
THE FINLEY FIRM, P.C.
3535 Piedmont Road
Building 14, Suite 230
Atlanta, GA 30305
Tel: (404) 320-9979
Fax: (404) 320-9978
Email: mgibson@thefinleyfirm.com

Jonathan S. Mann (ASB-1083-A36M)
(*pro hac vice forthcoming*)
Austin B. Whitten (ASB-7228-K13Y)
(*pro hac vice forthcoming*)
PITTMAN, DUTTON, HELLUMS, BRADLEY & MANN, P.C.
2001 Park Place North, Suite 1100
Birmingham, AL 35203
Tel: (205) 322-8880
Fax: (205) 328-2711
Email: jonm@pittmandutton.com
Email: austinw@pittmandutton.com

Attorneys for Plaintiff and the Proposed Class